K-system generator of pseudorandom numbers on Galois field [*]

G.G.Athanasiu
Physics Department,University of Crete
GR-71409 Iraklion, Crete, Greece

E.G.Floratos
National Research Center "Demokritos",
GR-15310 Ag. Paraskevi, Athens, Greece;
Physics Department,University of Crete,
GR-71409 Iraklion,Greece

G.K. Savvidy
National Research Center "Demokritos",
GR-15310 Ag. Paraskevi, Athens, Greece

Abstract

We analyze the structure of the periodic trajectories of the K-system generator of pseudorandom numbers on a rational sublattice which coincides with the Galois field $GF[p]$. The period of the trajectories increases as a function of the lattice size p and the dimension of the K-matrix d. We emphasize the connection of this approach with the one which is based on primitive matrices over Galois fields.

[*] Reprint DEMO-HEP 97/03 Feb.97

1 Introduction

Nowadays the Monte-Carlo method has a wide range of applications and the quality of pseudorandom numbers being used plays an important role. Different principles and algorithms have been suggested in the literature to generate pseoudorandom numbers and to check their properties [1]. The development of the ergodic theory [2, 3, 4, 5] and the progress in understanding of nonlinear phenomena together with the increasing power of modern computers open a new era for applications [7, 8, 9].

In the articles [10] the authors suggested to use many-dimensional Kolmogorov K-systems to generate pseudorandom numbers of high quality. K-systems are the most stochastic dynamical systems, with nonzero Kolmogorov entropy and their trajectories are exponentially unstable and uniformly fill the phase space [2, 3, 6, 12, 13, 10]. It was suggested to use the coordinates of these trajectories as a sequence of pseudorandom numbers [10]. From this point of view the most successful inversive congruential generator [1] used so far can be considered as a one-dimensional K-system and it was pointed out that this fact explains its exceptional properties [10].

For the application of this idea it is important to have such K-systems for which the phase space is limited by a unit d-dimensional torus, because in that case the coordinates of the trajectories can be used directly without any additional transformations. Two types of K-systems have been suggested for these purposes: toral automorphisms [10, 11] and many-dimensional Sinai billiard which is defined inside a unit d-dimensional torus [14].

In the case of toral automorphisms a unit d-dimensional torus Π^d plays the role of a phase space and the K-system is represented by a d-dimensional matrix - *K-matrix* - which acts on the vectors from Π^d generating trajectories uniformly distributed over the torus Π^d. The coordinates of these trajectories are used for Monte-Caro simulations [10, 11]. The properties of this new class of matrix generators were investigated by different criterion including Kolmogorov discrepancy D_N . In all cases it shows good statistical properties [11].

The aim of this article is to estimate the period of the trajectories which are used to produce pseudorandom numbers generated by a K-system. It is clear, that only periodic trajectories of K-systems can be simulated on a computer, because trajectories on a computer are always on a finite rational sublattice Z_p^d of the phase space Π^d. Thus we have to consider the system on rational sublattice Z_p^d of a unit d-dimensional torus and particularly on sublattices with *prime* basis p [23, 24, 25, 27, 26, 36, 32, 28]. These sublattices are equivalent to Galois fields $GF[p]$ and all four elementary arithmetical operations can be carried out unrestrictevely [21, 20, 22].

Analyzing trajectories of a K-system on a Galois sublattice $GF[p]$ one can see that in order to have trajectories with large period K-matrix should have an eigenvalues in high extensions $GF[\sqrt[d]{p}]$ of the field (notation used in mathematical literature is $GF[p^d]$). This property makes them very close to so called *primitive matrices* which have been considered by Niedereiter [16, 17] to generate pseudorandom numbers. We refer to the book of Niederreiter [19] and to the survey article [18] for recent references. The main idea of his approach is to use a primitive matrices on a given Galois field $GF[\sqrt[d]{p}]$ to generate pseudorandom numbers of very large periods. This approach guarantees the large period of the series. In addition the fascinating result of Niedereiter [18] allows to estimate the uniformity of maximally long trajectories in terms of Kolmogorov discrepancy D_N.

Thus these two approaches are very close to each other on Galois sublattices and the main question is: *whether one can have the matrices with both properties at the same time?* The determinant of a K-matrix should be equal to one while the determinant of a primitive matrix is different from one, thus *these properties are incompatible*. The main point, which we would like to stress here, is that nevertheless one can construct K-matrices which have a *primitive matrix as submatrices*. In that case the trajectories are still very long as in the case of primitive matrices, but at the expense of appearance of trajectories with short period. Excluding them from initial data we guarantee that the trajectories are maximally long and at the same time belong to a K-system. We suggest specific matrices with these properties which can be used for practical simulations.

2 Trajectories of K-system on a rational sublattice

Let us pass to the details of the algorithm. The matrix generator is defined as [10, 11],

$$X^{(n+1)} = A \cdot X^{(n)}, \qquad\qquad (mod\ 1), \tag{1}$$

where A is $d \times d$ dimensional matrix with integer matrix elements $a_{i,j}$ and determinant equal to one

$$Det\ A = 1, \tag{2}$$

and $X^{(0)} = (X_1^{(0)}, ..., X_d^{(0)})$ is an initial real vector. The last condition provides phase-space volume conservation. The automorphism (1) forms the K-system of Anosov if and only if all eigenvalues of the matrix A are in modulus different from unity [3, 4, 5]

$$|\lambda_i| \neq 1, \qquad i = 1, ..., d \tag{3}$$

The *trajectory* of the K-system (1)

$$X_0, X_1, X_2....$$

represents the desired sequence of the pseudorandom numbers [10].

This approach allows a large freedom in choosing the matrices A for the K-system generators and the initial vectors [10]. Specific choices suggested in [10, 11, 35] are

$$A_d = \begin{pmatrix} 2,3,4,.......,d\ \ ,1 \\ 1,2,3,.....,d-1,1 \\ 1,1,2,.....,d-2,1 \\ .... \\ .... \\ 1,1,1,...,2,3,4,1 \\ 1,1,1,...,1,2,2,1 \\ 1,1,1,...,1,1,2,1 \\ 1,1,1,...,1,1,1,1 \end{pmatrix}, A_d = \begin{pmatrix} 0,\ \ 1\ ,\ \ 0\ ,.....,\ \ 0 \\ 0,\ \ 0\ ,\ \ 1\ ,.....,\ \ 0 \\ .... \\ .... \\ 0,\ \ 0\ \ ,\ \ 0\ \ ,.....,\ \ 1 \\ (-1)^{d+1}, a_1, a_2, .., a_{d-1} \end{pmatrix}. \qquad (4)$$

The first matrix has the advantage to be well defined in any dimension d and it has a very large Kolmogorov entropy [10] which is given by the Anosov-Sinai formula

$$h(A_d) = \sum_{|\lambda_k|>1} ln\lambda_k.$$

The entropy h defines the number $\pi(\tau)$ of the periodic trajectories with period less or equal to τ [30, 31, 32]

$$\pi(\tau) \rightarrow \frac{e^{h\tau}}{h\tau}$$

when $\tau \rightarrow \infty$, thus the number of "available" trajectories increases with entropy. The second one has a very simple expression for its characteristic polynomial

$$\lambda^d - a_{d-1}\ \lambda^{d-1} - ... - a_1\ \lambda + (-1)^d =$$

and for its eigenvalues $\lambda_1, ..., \lambda_d$ we have $\lambda_1 \cdots \lambda_d = 1$,..., $\lambda_1 + ... + \lambda_d = a_{d-1}$. These formulas allow to choose eigenvalues and then to construct K-matrices. This correspondence between matrices and polynomials has a wide range of applications in algebra and number theory [20]. In the given case $DetA_d = 1$ to fulfil K-condition (2) [35].

Let us consider trajectories of the system (1) with an initial vector $X^{(0)}$ which has rational coordinates [23, 24, 25, 27, 26, 32, 28]

$$X^{(0)} = (\ \frac{q_1}{p_1},\ \ \frac{q_2}{p_2}, ..., \frac{q_d}{p_d}\ \ ). \qquad (5)$$

It is easy to see, that all these trajectories are periodic orbits of the Anosov map (1), because matrix elements $a_{i,j}$ are integer. Indeed, if we consider the sublattice of unit torus Π^d with rational coordinates of the form q/p where p is the least common multiple of p's

$$X = (\ \frac{q_1}{p},\ \ \frac{q_2}{p}, ..., \frac{q_d}{p}\ \ ), \qquad 0 \leq q_i \leq p-1$$

then the multiplication,summation and (mod) operations (1) will leave the trajectory on the same sublattice. The total number of vertices on this sublattice Z^d_p is

$$(total\ number\ of\ verteces) = p^d,$$

therefore the period τ_p of the trajectories on $Z_p^d = Z_p \otimes ... \otimes Z_p$, where $Z_p = \{0, 1, ..., p-1\}$ is always less than p^d

$$\tau_p \leq p^d.$$

Thus the periodic trajectories of this system (1) with the initial vector (5) coincide with a subset of the points of rational sublattice Z_p^d and our goal is to find conditions under which the period of the *K-system* will be as large as possible.

Let us show that on every given sublattice Z_p^d Anosov map (1) reduces to (mod p) arithmetic. Indeed on sublattice Z_p^d the Anosov map A (1) can be written as

$$\frac{q_i^{(n+1)}}{p} = \sum_j a_{i,j} \; \frac{q_i^{(n)}}{p}, \qquad\qquad (mod\ \ 1)$$

and is equivalent to (mod p) arithmetic on the lattice with integer coordinates q_i which are in the interval $[0, p-1]$

$$q_i^{(n+1)} = \sum_j a_{i,j} \; q_i^{(n)}, \qquad\qquad (mod\ \ p).$$

Thus the images of the periodic trajectories on a unit torus Π^d appear as trajectories on the integer sublattice Z_p^d and all operations can be understood (mod p). The most important thing is that now all operations become commutative.

To estimate the period of the trajectories on a rational sublattice it is essential to consider those sublattices for which p is the prime number, we mean that $p_1 = ... = p_d = p$ [23, 24, 25, 27, 26, 32, 28]. In that case the integer sublattice gains an additional structure and becomes the Galois field $GF[p]$ and all operations reduce to arithmetic ones on Galois field. The benefit to work on Galois field is that four arithmetic operations are well defined on that sublattice [21].

In this way we can consider every coordinate q_i , $i = 1, ..., d$ as belonging to Galois field $GF[p] = \{0, 1, ..., p-1\}$, where p *is a prime number* and consider the sublattice as a direct product of Galois fields.

$$Z_p^d = GF[p] \otimes ... \otimes GF[p].$$

As we already mentioned, this reduction of a dynamical system (1) to a dynamical system for which the Galois field plays the role of the phase space makes all operations commutative in the sense that

$$\{A\{A\ X\}\} = \{A^2\ X\},$$

where $\{...\}$ means mod operation. The commutativity of the multiplication and (mod) operation on the Galois sublattice means that the periodic trajectory

$$\{A\{A.........\{A\ X\}...\}\} = X$$

can be represented in the form

$$\{A^{\tau_p}\ X\} = X.$$

This equation allows to understand the relation between eigenvalues of the matrix A and the period of the trajectories. Indeed let us consider the eigenvalue problem for the matrix A on a Galois sublattice

$$A\ X = \lambda\ X, \tag{6}$$

then the period of the given trajectory τ_p can be understood as a degree of power on which the λ reduces to identity $(mod\ \ p)$

$$\lambda^{\tau_p} = 1 \qquad\qquad (mod\ \ p). \tag{7}$$

The period of the trajectory on a Galois sublattice $GF[p]$ is equal therefore to the power τ_p in which the eigenvalue of the matrix A reduces to identity. It is obvious that the same matrix A will have different periods on different Galois fields and that this period depends on the given prime number p,the dimension of matrices d and the initial vector X_0.

3 Eigenvalues of the generator and the period of the trajectories

Thus the actual value of the period τ_p naturally depends on the form of eigenvalues λ and of the prime number p. Here we can distinguish different cases:

i). The eigenvalue λ coincides with one of the elements of the Galois field $GF[p]$. In that case the period τ_p depends on the fact whether eigenvalue coincides with a primitive element of the Galois field. All elements of the field $GF[p]$ can be constructed as powers of primitive element g and $g^{p-1} = 1$. If the eigenvalue coincides with the primitive element of the Galois field ,

$$\lambda = g, \qquad where\ g\ is\ a\ primitive\ element\ of\ GF[p], \tag{8}$$

then the period is maximal and is equal to $\tau_p = p - 1$

$$\lambda^{p-1} = 1, \qquad (mod\ \ p). \tag{9}$$

Therefore to get the maximal period in the case i) one should have an eigenvalue equal to the primitive element g. If λ does not coincide with the primitive element g, then the period is simply smaller and is equal to $(p-1)/m$ where m is a divisor of $p-1$.

ii). The eigenvalue does not coincide with any element of the Galois field $GF[p]$. This may happen because Galois field is arithmetically complete, but it is not algebraically complete, therefore one can have the situation when the solution of the characteristic polynomial of the K-matrix is not in the field $GF[p]$. In that case one should ask, whether it is an element of the quadratic extension $GF[\sqrt{p}]$ or of higher extensions. The quadratic extension of the Galois field consists of the numbers of the form $a + b\sqrt{g}$ where a, b are the elements of field $GF[p]$, g is the primitive element of $GF[p]$ and $\sqrt{g}$ is a square-free integer. The primitive element of the $GF[\sqrt{p}]$ has the period equal to p^2-1 [21].

Thus if the eigenvalue is an element of the quadratic extension and coincides with its primitive element h

$$\lambda = h, \qquad where \quad h = h_1 + h_2\sqrt{g} \qquad is\ a\ primitive\ element\ of\ GF[\sqrt{p}], \quad (10)$$

then the period is equal to $\tau_p = p^2-1$

$$\lambda^{p^2-1} = 1, \qquad (mod \ \ p). \quad (11)$$

iii). In general the characteristic polynomial of the K-matrix is of order d and the eigenvalue may belong to high extensions $GF[\sqrt[d]{p}]$ of the Galois field. The elements of $GF[\sqrt[d]{p}]$ have the form $a+bh+...+eh^{d-1}$ where $a,b,...,e$ are the elements of $GF[p]$ and h is a primitive element of $GF[\sqrt[d]{p}]$ [20, 21, 22]. If the eigenvalue λ coincides with this primitive element

$$\lambda = h \quad where\ h\ is\ a\ primitive\ element\ of\ GF[\sqrt[d]{p}], \quad (12)$$

then the period is equal to $\tau_p = p^d-1$ [20, 21, 22]

$$\lambda^{p^d-1} = 1, \qquad (mod \ \ p). \quad (13)$$

This analysis demonstrates an important fact that in order to have a large period on a sublattice $GF[p]$ one should have K-matrices with eigenvalues in high extensions of the field.

4 Generators with largest period

In the previous sections we described the trajectories of the K-system on the rational sublattice Z_p^d and particularly on a Galois field, that is when p is a prime number. We have seen that the period of the trajectories depends on the "order" of the corresponding eigenvalue and the period is as large as the order of the extension of the field to which belongs the eigenvalue. The question is: can we construct a K-matrices with eigenvalues in high extensions of the Galois field and how many of them can *simultaneously* belong to a maximal extension $GF[\sqrt[d]{p}]$?

We should remark that the d-dimensional matrices A with *all* eigenvalues in $GF[\sqrt[d]{p}]$ are well known in number theory and correspond to so called *primitive matrices* of the field $GF[\sqrt[d]{p}]$ and *the determinant of primitive matrices is not equal to one* [20, 21, 22]. Therefore the K-matrices which have the determinant equal to one can not coincide with the primitive matrices, but as we will see one can construct K-matrices with $d-1$ eigenvalues in $GF[\sqrt[d]{p}]$ and only one in $GF[p]$. This means that most of the trajectories will have the maximal period $\tau_p = p^d-1$ and only few of them (corresponding to that exceptional eigenvalue) will have smaller period and we should exclude them from initial data.

First let us construct the K-matrices which have the eigenvalues in quadratic extension $GF[\sqrt{p}]$. If h is the primitive element of the $GF[\sqrt{p}]$, that is

$$h = h_1 + h_2\sqrt{g}, \qquad h \cdot h^{\star} = g, \quad h + h^{\star} = 2h_1, \tag{14}$$

then the matrix which has the eigenvalues in $GF[\sqrt{p}]$ can be constructed in the form of (4)

$$A_3 = \begin{pmatrix} 0, & 1, & 0 \\ 0, & 0, & 1 \\ -1, & 2h_1 g^{-} - g, & 2h_1 - g^{-} \end{pmatrix}, \quad (mod \;\; p) \tag{15}$$

because the characteristic equation is

$$(\lambda + g^{-})(\lambda - h)(\lambda - h^{\star}) =$$
$$\lambda^3 - (2h_1 - g^{-})\lambda^2 - (2h_1 g^{-} - g)\lambda + 1 = 0 \quad (mod \;\; p) \tag{16}$$

and has two roots in $GF[\sqrt{p}]$ and one root in $GF[p]$. The period of the most trajectories is equal to

$$\tau_p = p^2 - 1. \tag{17}$$

and is quadratic in p. At the same time the trajectories with the initial vector corresponding to eigenvalue $\lambda = -g^{-}$ are smaller and one should exclude them from initial data. It is also easy to see that if we want to construct two-dimensional K-matrices with eigenvalues only in $GF[\sqrt{p}]$ we face the problem with determinant $Det\ A = h \cdot h^{\star} = g \neq 1$. This observation explains why two-dimensional K-systems, like Arnold cat, can not have periodic trajectories of the length $p^2 - 1$ on any Galois sublattice.

To construct a K-matrix generator with eigenvalues in high field $GF[\sqrt[d]{p}]$ we will use primitive polynomial of degree d over $GF[\sqrt[d]{p}]$. The primitive polynomial has the form [21, 20, 22]

$$\lambda^d + \beta_1\lambda^{d-1} + \beta_2\lambda^{d-2} + ... + \beta_d = 0 \tag{18}$$

with coefficients $\beta_1, \beta_2, ..., \beta_d$ over $GF[p]$. The roots of this characteristic polynomial coincide with different powers of a primitive element h (12) of $GF[\sqrt[d]{p}]$

$$\lambda_1 = h, \quad \lambda_2 = h^p, \quad ... \quad , \lambda_d = h^{p^{d-1}}$$

If $p^d - 1$ is not divisible by $p,\ p^2, ..., p^{d-1}$, then all of them are primitive elements of $GF[\sqrt[d]{p}]$. This is the reason why this polynomial is called "primitive". There are two equivalent representations of h: i) in the form of root of the polynomial (18) and ii) in the form of corresponding matrix [21, 20, 22]

$$A_d = \begin{pmatrix} 0, \;\; 1 \;, \;\; 0 \;, ..., \;\; 0 \\ 0, \;\; 0 \;, \;\; 1 \;, ..., \;\; 0 \\ .... \\ .... \\ 0, \quad ... \quad 0 \quad , \quad 1 \\ -\beta_d, \quad ..... \quad , -\beta_2, \quad - \beta_1 \end{pmatrix} \quad (mod \;\; p). \tag{19}$$

As we already explained the problem is that the primitive polynomial (18) and the corresponding primitive matrix (19) do not have determinant equal to one, because $\beta_d \neq 1$. But this property is incompatible with K-condition (2). The exceptional case is only $GF[2]$.

Nevertheless one can solve this problem as follows: the last term β_d which is equal to the determinant of the primitive matrix coincides with the primitive element g of $GF[p]$ $\beta_d = g$, therefore if we multiply the primitive polynomial (18) by $\lambda + g^-$ we will get the polynomial

$$\begin{gathered}(\lambda + g^-)(\lambda^d + \beta_1\lambda^{d-1} + \beta_2\lambda^{d-2} + ... + \beta_d) = \\ \lambda^{d+1} + (\beta_1 + g^-)\lambda^d + (\beta_2 + \beta_1 g^-)\lambda^{d-1} + ... + 1 = 0.\end{gathered} \qquad (20)$$

to which corresponds a matrix with unit determinant of the form (4)

$$A_{d+1} = \begin{pmatrix} 0, & 1\,, & 0\,, \ldots\ldots\ldots\ldots\ldots\ldots, & 0 \\ 0, & 0\,, & 1\,, \ldots\ldots\ldots\ldots\ldots\ldots, & 0 \\ & & \ldots\ldots\ldots & \\ & & \ldots\ldots\ldots & \\ 0, & \ldots & 0 \qquad , & 1 \\ -1, \ldots.., & -(\beta_2 + \beta_1 g^-), & & -(\beta_1 + g^-) \end{pmatrix} \quad (mod \;\; p). \qquad (21)$$

of dimension $d+1$. The trajectories generated by this matrix will have the period

$$\tau_p = p^d - 1 \qquad (22)$$

and we should exclude "dangerous" trajectories corresponding to eigenvalue $\lambda = -g^-$. They have the form $X^{(0)} = (x_1, \; x_1(-g^-), ..., x_1(-g^-)^d)$ and very short period $(p-1)/2$.

Fascinating result of Niedereiter [18] allows to estimate the uniformity of maximally long trajectories in terms of Kolmogorov discrepancy D_N

$$\frac{D_{\tau_p}}{\tau_p} = \frac{1}{\tau_p + 1}.$$

The result is very important because the convergence of the Monte-Carlo simulations essentially depends on D_N [10].

The example of the primitive polynomial on $GF[\sqrt[d]{7}]$ with $d = 10$ is [20] $\lambda^{10} + \lambda^9 + \lambda^8 + 3 = 0$ and (20) has the form $\lambda^{11} - \lambda^{10} - \lambda^9 - 2\lambda^8 - 4\lambda + 1 = 0$ therefore the matrix is

$$A_{11} = \begin{pmatrix} 0, \;\; 1\,, \;\; 0\,, \ldots.., \;\; 0 \\ 0, \;\; 0\,, \;\; 1\,, \ldots.., \;\; 0 \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ 0, 0, 0, ..., 0, 0, 0, 1 \\ -1, 4, 0, ..., 0, 2, 1, 1 \end{pmatrix} \qquad (mod \;\; 7) \qquad (23)$$

and the trajectories have the period $7^{10} - 1$ except of two trajectories with the initial vectors of the form $X^{(0)} = (1, 2, 4, 1, 2, 4, 1, 2, 4, 1, 2)$ and $X^{(0)} = (3, 6, 5, 3, 6, 5, 3, 6, 5, 3, 6)$. The same matrix will have different properties on Galois field $GF[p']$ where $p' \neq p$.

The determination of the set of primes for which a given matrix has the maximal period is an unsolved problem [33].

Tables of primitive polynomials with large values of d are available [20]. In particular [37] contains tables for $d < 101$, in [38] for $d < 169$ and in [39] for $d < 1001$ with the corresponding periods of order 2^{1000}.

4.1 Conclusion

In this article we advocate two approaches to generate pseoudorandom numbers of high quality: i) the first one is based on K-system generators with their exponentially unstable trajectories uniformly filling the phase space and ii) on primitive matrices acting on a given Galois sublattice with their maximally long trajectories. We demonstrate that one can combine these properties in a unique K-matrix which has primitive matrix as a submatrix. This construction guarantees that the trajectories belong to a K-system and at the same time have maximally large periods.

Acknowledgments

We are thankful to N.Akopov for his interest and discussions in the early stages of this work.

References

[1] D.E.Knuth. The art of computer programming. vol. 2. Seminumerical algorithms (Addison-Wesley, Reading, MA, 1969)

[2] A.N.Kolmogorov, Dokl.Akad.Nauk SSSR 119, 861 (1958)

[3] D.V.Anosov, Geodezicheskiye Potoki na Zamknutych Rimanovych Mnogoobraziyach Otrizatelnoi Krivizny (Geodesic flows on closed Riemannian manifolds of negative curvature) (Nauka, Moscow, 1967).

[4] V.A.Rohlin. Uspechi Mat.Nauk 4 (1949) 47
Izv.Akad.Nauk SSSR. Ser.Mat. 13 (1949) 329; 25 (1961) 499
Russian Math. Surveys 15 (1960) 1

[5] Ya.G.Sinai. Dokl.Akad.Nauk SSSR 124 (1959) 768

[6] I.P.Kornfeld, S.V.Fomin, Ya.G.Sinai, Ergodic theory (Springer-Verlag, New York, 1982) (Engl.transl).

[7] M.Creutz, Quarks, gluons and lattices. (Cambridge University Press,Cambridge 1983)

[8] J. Ambjørn, Quantization of Geometry, in: Fluctuating Geometry in Statistical Mechanics and Field Theory, (Les Houches, Session LXII, 1994) Nucl.Phys. B451 (1996) 643.

[9] J. Ambjorn and K.N. Anagnostopoulos (Bohr Inst.). NBI-HE-96-69, Dec 1996. 38pp. e-Print Archive: hep-lat/9701006

[10] G.K.Savvidy and N.G.Ter-Arutyunian, On the Monte-Carlo Simulation of Physical Systems, J.Comput.Phys. 97, 566 (1991);
Preprint EPI-865(16)-86, Yerevan Jun.1986.

[11] N.Z.Akopov,G.K.Savvidy and N.G.Ter-Arutyunian, Matrix Generator of Pseudorandom Numbers, J.Comput.Phys.97, 573 (1991);
Preprint EPI-867(18)-86, Yerevan Jun.1986;

[12] G.K.Savvidy, Nucl.Phys.B246, 302 (1984).

[13] G.K.Savvidy.Phys.Lett.130B, 303 (1983).

[14] R.O.Abramyan, N.Z.Akopov, G.K.Savvidy and N.G.Ter-Arutyunian, Sinai Billiards as a Pseudorandom Number Generator, Preprint EPI-922(73)- 86, Yerevan 1986;
G.A.Galperin, N.I.Chernov.Billiardi i Chaos. Matematika i Kibernetika 5, 10 (1991), (Znanie, Moskva, 1991).

[15] N.Z.Akopov, G.G.Athanasiu, E.G.Floratos and G.K.Savvidy. Preprint CRETE.TH/12/95; hep-lat/9601003.

[16] H.Niederreiter. Math. Japonica 31, 759 (1986).

[17] H.Grothe. Zufallszahlen und Simulation (Teubner, Stuttgard, 1986); Statist. Papers 28, 233 (1987).

[18] H.Niederreiter.Random Number Generation and Quasi-Monte Carlo Method. SIAM, Phyladelphia, 1992

[19] H.Niederreiter. Finite fields, pseudorandom numbers, and quasirandom points, in : Finite fields, Coding theory, and Advance in Communications and Computing. (G.L.Mullen and P.J.S.Shine, eds) pp. 375-394, Marcel Dekker, N.Y. 1993.

[20] R.Lidl and H.Niederreiter. Finite Fields, vol 20, Encyclopedia of Mathematics and its Applications, (Cambridge U.P., Cambridge, 1983)

[21] T.M.Apostol. Introduction to Analytic Number Theory. Springer-Verlag N.Y. 1984.

[22] J.R.Bastida. Field Extensions and Galois Theory, vol 22, Encyclopedia of Mathematics and its Applications, (Cambridge U.P., Cambridge, 1984)

[23] J.H.Hannay and M.V.Barry, Physica 1D (1980) 267.

[24] I.Percival and F.Vivaldi, Physica 25D (1987) 105.

[25] F.Vivaldi and S.Hatjispyros, Nonlinearity 5 (1992) 961;
F.Vivaldi, Nonlinearity 5 (1992) 133

[26] M.Bartuccelli and F.Vivaldi, Physica D 39 (1989) 194

[27] F.J.Dyson and H.Falk, Period of a discrete cat mapping. (1992) 603

[28] G.G.Athanasiu and E.G.Floratos, Nucl.Phys. B425 (1994) 343;
Polar decomposition of primitive elements in $GF[p^2]$,
Crete University preprint CRETE.TH/9/93

[29] G.G.Athanasiu,E.G.Floratos and S.Nicolis, Holomorphic quantization on the torus and finite quantum mechanics, Preprint LPTENS 95/43; hep-th/9509098

[30] Ya.Sinai, Trans.Amer.Math.Soc. 73 (1968) 227

[31] W.Parry and M.Polilcott, Ann.Math. 118 (1983) 573

[32] M.D.Esposti and S.Isola, Nonlinearity 8 (1995) 827

[33] J.P.Keating. Nonlinearity 4 (1991) 277

[34] N.Z.Akopov, E.M.Madunts, G.K.Savvidy, A new matrix generator for lattice simulation, in Proceedings of Computing in High Energy Physics'91 International Conference, pp.477-479 (Tsukuba, Japan, 1991).

[35] N.Z.Akopov, E.M.Madunts,A.B.Nersesian, G.K.Savvidy and W.Greiner, Fast K-system generator of pseudorandom numbers. in Proceedings of the XXVIII International Symposium Ahrenshoop, pp.281-286 (Wendisch-Rientz, Germany, 1994)

[36] P.Cvitanovic,I.Percival and A.Wirzba. Quantum Chaos-Quantum Measurement. (Kluwer Academic, 1987)

[37] E.J.Watson, Primitive polynomials (mod2). Math.Comp. 16 (1962) 368

[38] W.Stahnke, Primitive binary polynomials, Math.Comp. 27 (1973) 977

[39] N..Zierler and J.Brillhart, On primitive trinomials (mod 2), Inform. and Control 13 (1968) 541; 14 (1969) 566